ABSTRACT

In a distributed sensor network, a method of key management is carried out in several phases, particularly key pre-distribution phase, shared key discovery phase, and as needed, a path key establishment phase. In the key pre-distribution phase, prior to DSN deployment, a ring of keys is distributed to each sensor node, each key ring consisting of randomly chosen keys from a large pool of keys which is generated off-line. A shared key exists between each two key rings with a predetermined probability. In the shared key discovery phase, which takes place upon deployment of the DSN, every sensor node discovers its neighbors in wireless communication range with which it shares keys, and the topology of the sensor array is established by forming secure communication links between respective sensor nodes. The path key establishment phase assigns a path key to selected pairs of sensor nodes in wireless communication range that do not share a key but are connected by two or more links at the end of the shared key discovery phase. The key management scheme also assumes a revocation phase for removal of the key ring of the compromised sensor node from the network. Also, re-keying phase is assumed for removal of those keys with the expired lifetime.